Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

1.2.1.3.3 Ensuring High Availability of the NPAC/SMS

The NPAC/SMS is a high availability system, consistently operating at or above 99.9% availability over the past 5 years. At the application level, several architectural and functional aspects contribute to this availability:

1. **Multi-Process, Multi-Machine Architecture**—This architecture means that, in most cases, if a process stops or if even an entire machine stops, the system continues to run.
2. Security-Related Information
3. **Process Management**—This feature provides NPAC/SMS-specific automated oversight of all processes, restarting a process if it ever stops. The use of shared memory allows the NPAC/SMS to retain important information that otherwise would have been lost when the process stopped.
4. Security-Related Information

Security-Related Information

1.2.1.3.4 NPAC/SMS Special Features

While the primary function of the NPAC/SMS is to manage information related to telephone numbers, the system offers a wide array of functionality that both complements basic transactions and improves the quality of the overall ecosystem. What follows is a brief overview of these features.

Synchronization

One of the most important functions of the NPAC/SMS is to ensure the local systems are in synch with the NPAC/SMS data. The integrity of the U.S. communications network relies on all SPs having the same addressing information, at the same time in order to properly route voice calls as well as SMS/MMS messages. To this end, the NPAC/SMS provides many different mechanisms to ensure synchronization among all communications SPs.

- Security-Related Information

- **Bulk Data Download (BDD)**—These files provide local systems the ability to re-create or update their databases based on data extracts taken from the NPAC/SMS. BDD files are available for all types of NPAC data (SV, pooled block, network data, Service Provider, notifications). These files can be generated based on activity in a certain timeframe, or for the entire database.
- **Automated Resend**—During overnight hours, the NPAC/SMS looks for local systems that are still on the failed list for SVs or pooled blocks and resends the downloads of these objects. We designed this feature to examine previous failure reasons and if the error indicates that a modify download was failed because the record does not exist in the local system, the NPAC will broadcast a Create operation rather than a download.
- **Audits**—The NPAC/SMS queries the LSMS systems for a specified set of telephone numbers, and compares the responses to its own data. Discrepancies are noted in an audit report, and corrective downloads are sent to any discrepant LSMS systems.

Mass Update/Mass Port

Service Providers often have a need to port large volumes of numbers in a controlled manner but require assistance to manage this process. The mass update/mass port tool was developed to provide this assistance. Mass update/mass port transactions can be defined for all types of NPAC/SMS operations (create, release, activate, modify, disconnect, and cancel).

Many options are available to control the execution of the job, including an ability to control the start time and to suppress notifications that normally would be generated. Several types of reports are available to monitor the progress and results of each job.

The mass update/mass port subsystem uses a scheduler process and a system of quotas to ensure all work is done in a fair and orderly fashion at reasonable volumes. The broadcast quota system is quite complex, and considers the following aspects when running "jobs".

- Whether the job will produce SV downloads, Pooled Block downloads, or no downloads at all
- The hour of the day the job is running;
- The day of the week the job is running; and
- Whether the job is being run by a provider or NPAC personnel.

The mass update/mass port subsystem also includes a dashboard that allows administrators to determine available broadcast quota and view projected completion times for jobs.

Optional Fields

Over time, the Industry has been interested in adding new types of data to the NPAC. However, this was a difficult process, largely because changes to the CMIP interface required many resources for development and testing.

To address this issue, Neustar developed the concept of optional fields. With this feature, a one-time change to the CMIP interface was made to add a new string to several of the existing CMIP messages. This string takes the form of an Security-Related Information that conforms to an Industry-approved schema that defines additional data fields. With this mechanism, a new field can be added to the NPAC without changing the CMIP interface definition.

The implementation of these fields in the NPAC is done dynamically, such that adding a new field requires minimal development and can be implemented during a maintenance window.

Pseudo-LRN

Pseudo-LRN (pLRN) provides a mechanism to add records to the NPAC that do not have an LRN associated with it. By using a specially tagged LRN value, these records are identified as pLRN and are broadcast only to systems that have opted in to receive pLRN records. Providers can opt in to all pseudo-LRN records or only for pseudo-LRN records from a certain set of providers.

OpGUI

The NPAC/SMS is a very complicated system that can process millions of requests in a single day. Many of these requests have service level requirements that must be met to fulfill the expectations of our customers. Management of this system could prove to be a challenge, but Neustar has built an infrastructure that has allowed the NPAC administrators to successfully manage the system for many years. This infrastructure includes an administrative interface, called the OpGUI, which provides functionality required to configure and maintain the NPAC/SMS. The OpGUI provides the following functionality for a system administrator to manage the NPAC/SMS:

1. **Managing NPAC Customer Profiles**—provides the capability to add, remove and modify NPAC Customers, configure their tunable options, configure their CMIP network access, and establish service bureau relationships.
2. **System Administrator Reports**—provides system administrators the ability to generate reports for needed to manage and tune the NPAC/SMS.
3. **Mass Update/Mass Porting (MUMP) Management**—provides system administrators the capability to manage all mass update and mass porting jobs that Service Providers ask the NPAC to perform on their behalf. These functions include creating, removing and updating MUMP jobs, projects, quotas, and profiles, as well as generating MUMP reports.
4. Security-Related Information
5. **User Administration**—allows NPAC administrators to add, remove, and update accounts that grant access to the NPAC OpGUI.

6. **System Parameter Management**—allows NPAC administrators to view and update the hundreds of system level parameters provided by the NPAC/SMS.

7. **CMIP Gateway Configuration**—allows NPAC administrators to configure the processes that provide the NPAC CMIP interface. These functions include assigning provider's systems to specific CMIP gateway processes and managing the parameters associated with the CMIP gateway.

8. **Billing Collection Configuration**—allows NPAC administrators to configure the information that is collected by the NPAC/SMS for billing purposes.

In addition to the OpGUI, Neustar has also built tools that provide a real-time view into what each NPAC region is processing and how well it is handling the load. Among these tools is the Security-Rela that provides a detail view into the Dispatcher Module that directs the messaging for a region. From this tool an administrator can see all messages being routed through the system and what process is working the request. Each request received by the NPAC/SMS may pass through as many as four processes. It's necessary to understand this traffic flow to ensure the NPAC/SMS is meeting the service level requirements associated with response time and SOA/LSMS interface performance.

Another administrative tool Neustar has built is the Security-Related Information . This tool provides a real-time cross-regional display of the key metrics related to NPAC/SMS performance and reliability. The Security-Ro provides two columns of metrics for each NPAC region. There is a metric delta column and a metric cumulative column for each of the following key metrics.

- Monthly, daily, and five-minute SLR 3 pass, failed, and percentage passed
- Monthly SLRs 5 and 6 pass, failed, and percentage passed
- Partial failure counts for subscription versions
- Database performance including average query, rollback, and commit times
- Count of SOA or LSMS systems in recovery
- Rules engine processing active and backlog queues
- CMIP interface active queue for each SOA/LSMS
- Count of long running requests
- Machine load for the application server machines
- Count of running NPAC/SMS processes

Another key feature that contributes to our successful management of the NPAC/SMS is the multitude of **dynamically configurable settings** that control system behavior. Neustar engineers have developed this capability to make it easier to manage the multitude of options offered by the NPAC/SMS, as well as, to easily extend the service for new functionality. Settings can be defined at several different levels, including at the interface level, at the provider level, and at the overall system level. For example, we can configure the duration of medium timers at the system level, but also configure whether a particular SOA supports medium timers. The NPAC/SMS has more than

500 such settings that can be changed without requiring the system to be restarted. When a setting is changed the different modules and processes in the system automatically detect the change and make necessary adjustments. This allows the NPAC administrators that are monitoring the system to make adjustments on the fly to meet the load placed on the system each day.

1.2.1.4 NPAC/SMS Database Layer

The Database Layer is between the Application Layer and the SAN Layer. It utilizes Security-Related Information operating on high availability Security-F database servers dedicated to each region. A DBMS is a set of programs that allows one to add, modify, and delete data in a database and to query it. It also provides methods for maintaining the Security-Related Information The application servers interact with the DBMS to ensure that data stored in the SAN is up to date and accurate.

Security-Related Information

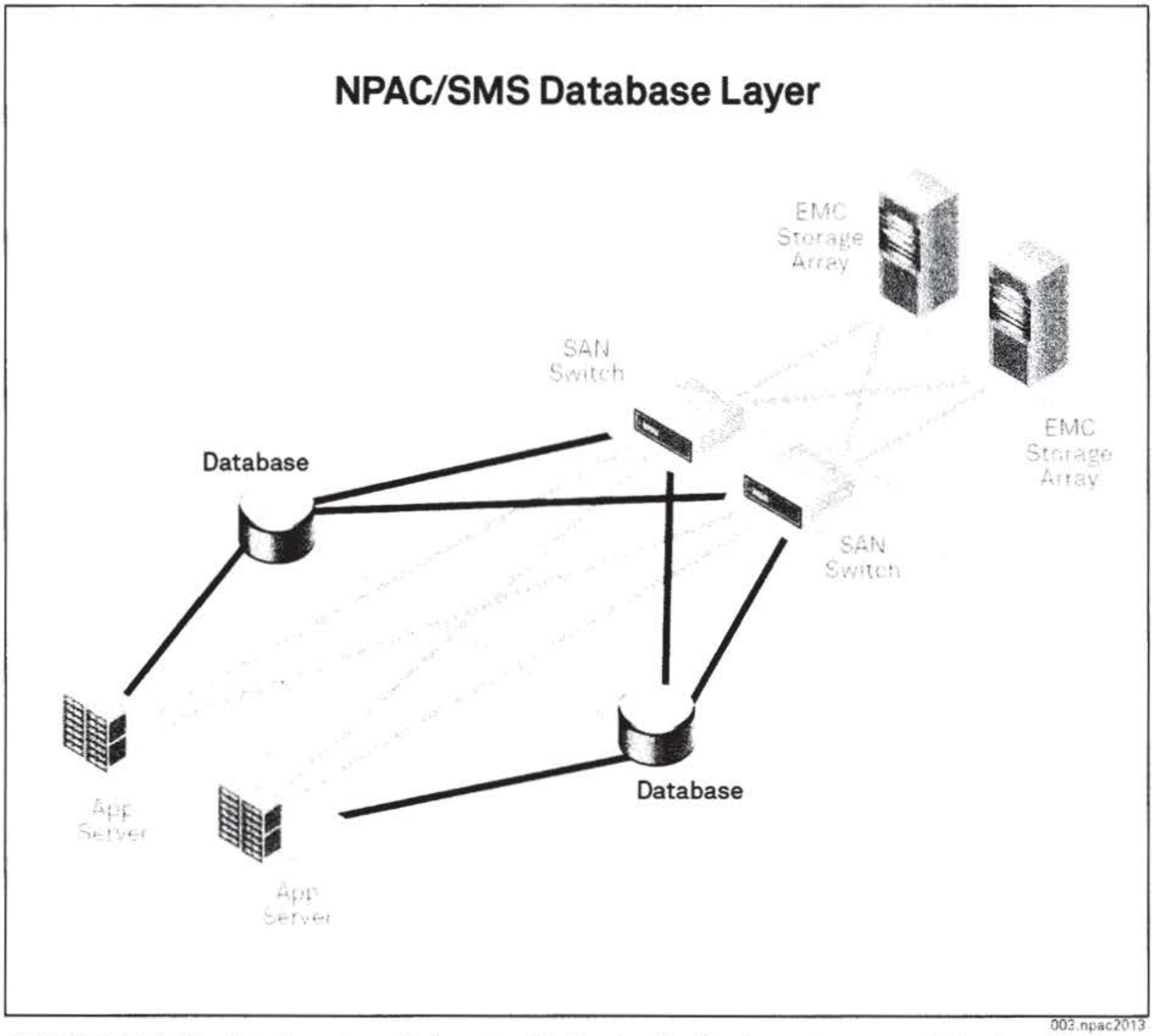
Database Layer Hardware and Software

The DBMS manages the storage of the NPAC's active and historical SV records. It also manages the storage of reporting data, logs and transient data, and data stored during the processing of a transaction.

Each region has its own Security-Related Information . Each server has 4 processors and 32 gigabytes of memory. The sole purpose of these servers is to run Security-Related Information Server product. We operate the software in Security-Related Information . Security-Relate is the Industry leader in providing database technology to transactional applications such as the NPAC/SMS. Security-Related Inf Each data center can fail over to the other in the event of an outage that requires this level of response.

Security-Related Information

The NPAC/SMS databases are reviewed yearly for SOX compliance to verify adequate internal control structure and procedures are maintained.



003.npac2013

Exhibit 1.2.1-9: **The Database Layer interacts with the Application Layer to ensure data stored in the SAN is up to date and accurate.**

Security-Related Information

Neustar has operated the NPAC/SMS with spectacular results in consideration of SLR performance, system availability and data consistency. For the new NPAC contract, four SLRs related to throughput and response time have been increased—SLR-1, Service Availability; SLR-4, LSMS Broadcast Time; SLR-5, SOA to NPAC Interface Rates; and SLR-6, NPAC to LSMS Interface Rates. All of these SLRs are dependent on highly efficient interaction of the Application and Database Layers. We know that the system as currently configured would not consistently meet these new levels. We will have to make further changes at both the Application Layer and the Database Layer to meet the new SLRs. Given our years of experience working internally and with our vendors to improve NPAC/SMS performance, we are confident that we will be able to fine-tune the NPAC/SMS to meet these new SLRs and the high service quality that the NPAC/SMS demands

Security-Related Information

Over the past 15 years, we have assembled a cross-functional team of network engineers, database experts, and systems architects to analyze the database traffic that comes from the database and optimize the data transmission settings at both the Network and Database Layers. Through intensive lab testing and consultation with experts from the database vendor, Security-Relate, we have been able to tune settings such as network send and receive buffers, as well as Security-Related Information to arrive at optimal settings for the NPAC's unique traffic patterns. These efforts produced dramatic improvements in minimizing the effects of the high latency imposed by the disparate databases.

Performance

Neustar makes use of many Security-Related features to ensure the database performs optimally. Examples include: locally managed tablespaces, automatic segment space management, automatic undo management, automatic memory management, SQL (structured query language, a language for managing data in databases) Baselines, and SQL Plan Management.

Additionally, Neustar has taken the extra architectural step to ensure high performance for NPAC users by separating out a reporting database. All the reporting workload reports requested by NPAC users such as daily Bulk Data Download (BDD) are executed against this reporting database so the performance based SLRs are met in the production NPAC/SMS database. Table 1.2.1-3 describes each of these features and their benefits.

Table 1.2.1-3. Features and Benefits of NPAC/SMS Reporting Database

Feature	Benefits
[redacted]	[redacted]
Automatic segment space management	Provides more efficient space utilization
[redacted]	[redacted]
Automatic memory management	Significantly simplifies Security-Related database administration by introducing a more dynamic, flexible, and adaptive memory management scheme
[redacted]	[redacted]
SQL plan management	Provides a mechanism for maintaining consistent SQL performance regardless of changes in optimizer version, optimizer statistics, schema changes, system settings and SQL profile creation
[redacted]	[redacted]

Security-Related Information

Security-Related Information

Security-Related Information

1.2.1.5 NPAC/SMS Storage Area Network (SAN) Layer

Neustar uses a Storage Area Network (SAN) to supply disk storage for the application and database servers. For the NPAC/SMS, we have engineered and deployed a SAN specifically designed for the Industry's stringent requirements.

Storage Area Network (SAN)

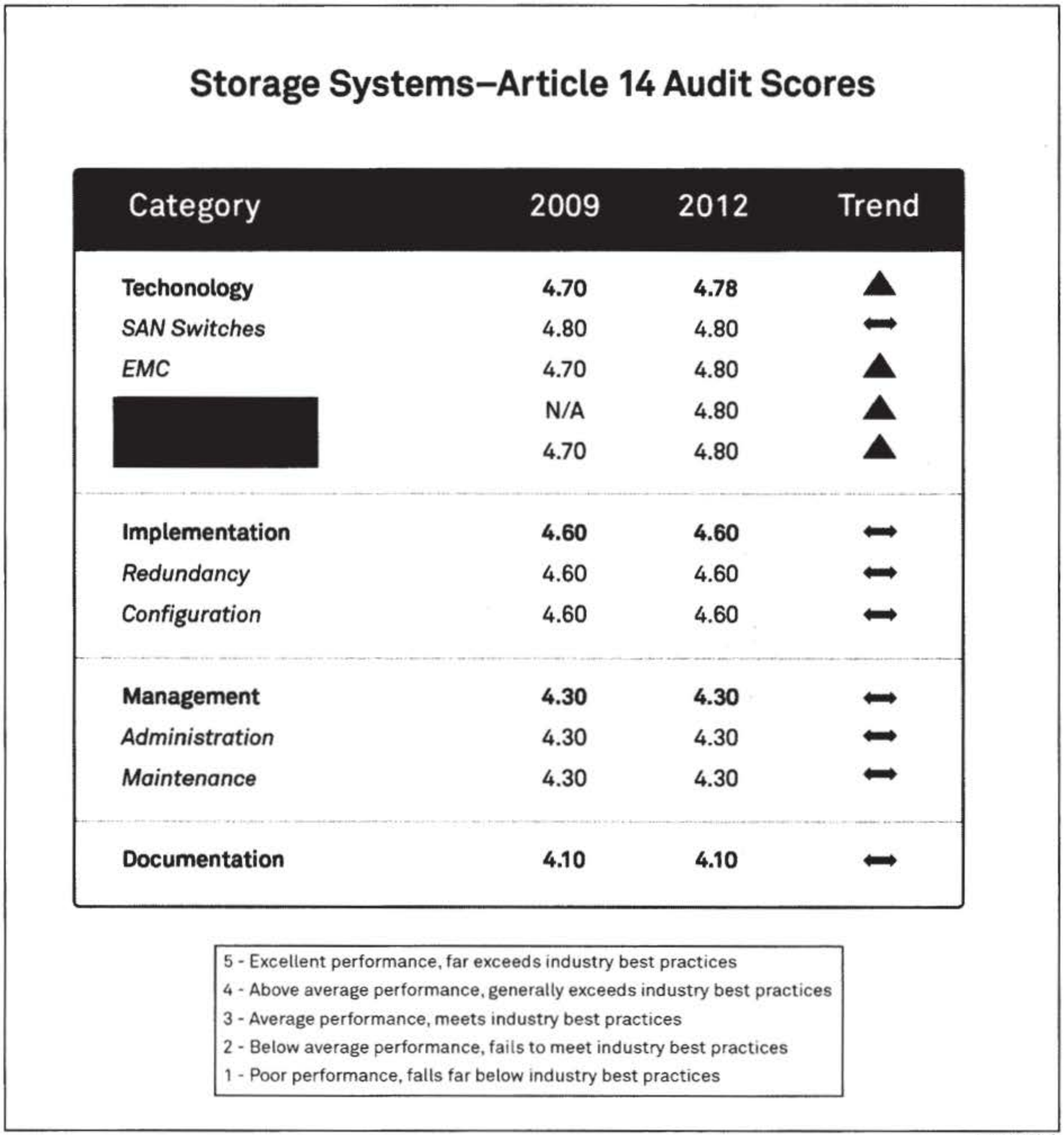
At a high level, a SAN provides storage in such a way that the storage appears to be locally attached to the server. The operating system communicates with SAN storage in much the same way that it would communicate with internal disk drives. Moving storage internal to the server to an external SAN provides many advantages, particularly with respect to availability, performance, and scalability. Thus, it is common for large-scale, complex applications like NPAC/SMS to use SAN storage.

Neustar's has designed the NPAC/SMS SAN Layer (shown in Exhibit 1.2.1-11) to maximize reliability, availability, and serviceability (RAS) characteristics.

1. **Reliability**—Properly instrumented storage solutions utilize self-diagnostics to provide indications of fault or problem prior to a major failure. This ensures data integrity and service performance even when an individual component fails.

2. **Availability**—Storage systems with built in redundancy allow for consistently higher uptime that is necessary to achieve four and five nine's level of availability. This allows us to predict failures and route around damaged components before any application impact occurs.

3. **Serviceability**—The simplicity and speed with which the storage unit can be maintained or repaired directly impacts uptime. A highly serviceable system is designed to be easy to work on, and automated where ever possible.



Storage Systems–Article 14 Audit Scores

Category	2009	2012	Trend
Techonology	**4.70**	**4.78**	▲
SAN Switches	4.80	4.80	↔
EMC	4.70	4.80	▲
[redacted]	N/A	4.80	▲
[redacted]	4.70	4.80	▲
Implementation	**4.60**	**4.60**	↔
Redundancy	4.60	4.60	↔
Configuration	4.60	4.60	↔
Management	**4.30**	**4.30**	↔
Administration	4.30	4.30	↔
Maintenance	4.30	4.30	↔
Documentation	**4.10**	**4.10**	↔

5 - Excellent performance, far exceeds industry best practices
4 - Above average performance, generally exceeds industry best practices
3 - Average performance, meets industry best practices
2 - Below average performance, fails to meet industry best practices
1 - Poor performance, falls far below industry best practices

146.npac2013

Exhibit 1.2.1-10: Third-party audits validate our performance and provide valuable input on possible future enhancements.

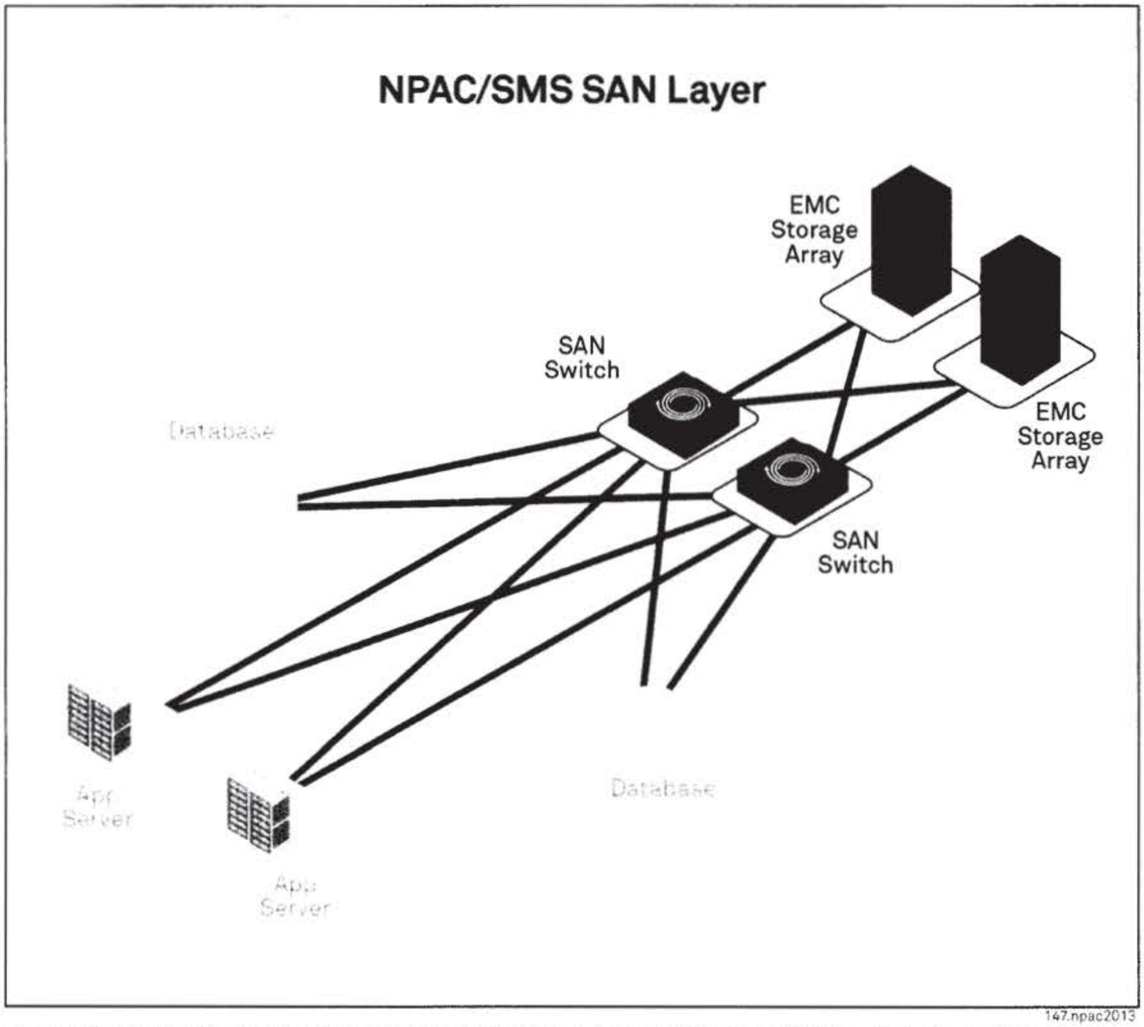


Exhibit 1.2.1-11: **The Application Layer and Database Layer utilize the SAN for disk storage to ensure higher availability and stability.**

The SAN Layer is comprised of two major components.

1. **Storage Arrays**—provides disk storage to all hosts in the NPAC/SMS
2. **SAN Switches**—connects all NPAC/SMS servers to Storage Arrays

Storage Arrays

Neustar always utilizes established technologies for the NPAC/SMS. The Storage Arrays used are EMC VMAX arrays, fully dedicated to the NPAC/SMS. This technology choice provides significant benefits to NPAC users because they are:

- Fault-tolerant
- Highly scalable, should the need arise
- Extremely high-performance and predictable in response time
- Highly instrumented, providing extensive proactive and predictive failure analysis
- Supported by an excellent Field Services organization that understands highly demanding applications

Security-Related Information

Table 1.2.1-4. VMAX Storage Array Protection Areas

Protection	Purpose
Security-Related Information	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
6. Standby power supply (batteries)	Enables controlled power off ensuring data integrity
[redacted]	[redacted]

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Offline Storage

Neustar uses multiple means to ensure continuous availability of the NPAC/SMS. As discussed in other sections of this document, the NPAC/SMS data is continuously replicated from the primary to the secondary data center, ensuring availability of the NPAC/SMS and guarding against data loss. In addition to using data replication to avoid data loss, Neustar also creates offline media (backup) copies of the NPAC/SMS databases, as an additional means of protecting the NPAC/SMS data. These offline copies are isolated from the primary operational systems, in accordance with Industry best practices.

The offline media copies are stored in a secure, off-site location, provided by a Tier 1 records management firm. Neustar ensures that there is a secure, auditable chain of custody for NPAC/SMS media from the time any media is created, to the time of storage in off-site facilities, to the time the media may be returned to Neustar to be restored.

Security-Related Information

Neustar performs regular test restores of NPAC/SMS data, ensuring systems and procedures are working correctly.

Staff and Operational Procedures

Neustar invests heavily in ensuring our staff is fully trained on the SAN assets for the NPAC/SMS and we employ ITIL compliant processes and procedures in managing and maintaining our SANs. The Storage team manages the NPAC/SMS SAN using Industry best practices, ensuring that all of the components are properly monitored and maintained and that new software is carefully tested before implementation. Neustar has rigorous change management procedures designed to ensure that operational changes are thoroughly planned and executed via a repeatable process.

The Neustar Difference

The SAN Layer provides extremely high-availability storage to all NPAC/SMS hosts. The arrays and switches within the SAN are highly redundant, and specifically selected to maximize reliability, availability, and serviceability. In addition, Neustar employs highly effective change management practices and procedures to ensure that the SANs have proper proactive maintenance and capacity planning necessary to meet the relevant NPAC/SMS SLRs (e.g., 99.99% availability of the NPAC/SMS).

The NPAC/SMS Storage Network Layer is audited ever year by TMNG. As shown previously in Exhibit 1.2.1-10, Neustar is consistently scored above 4.5 out of 5. A score of 4 is considered "Above average performance, generally exceeds Industry best practices" and a 5 is considered "Excellent performance, far exceeds Industry best practices".

1.2.2 NPAC/SMS Functionality

In the decade and a half since the inception of the NPAC, the system has evolved to offer a wide array of capabilities that benefit the provider community. As the NPAC Administrator during this entire period, Neustar has aggressively and responsibly fostered the advancement of new or improved functionality within the NPAC system. Further, Neustar maintains a vision for the NPAC into the future to continue this record of constant improvement.

The NPAC/SMS is a key component of the NPAC service and has evolved significantly over the last 15 years. NPAC/SMS functionality is developed in partnership with the Industry through various committees under the auspices of the NANC (for example, the LNPA WG).

In this section we describe the functionality that enables NPAC transactions, administrative functionality required to operate the service, and new functionality for the next term that are either proposed by Neustar or referenced in the RFP with the potential to improve value for the Industry.

[redacted]	
Administrative Functionality	• Mass Update and Mass Port • Billing • Reporting
Security-Related Information	

1.2.2.1 Functionality that Enables NPAC Transactions

Subscription Version Processing

The majority of code in the Security-Related Information provides functionality that enables NPAC/SMS transactions. Records created in the NPAC/SMS by the users are called subscription versions (SV). SV processing can be divided into four main categories:

1. Enforcement of business rules
2. Data validations
3. Dissemination of data
4. Synchronization

Enforcement of NPAC/SMS Business Rules

Processing an NPAC/SMS transaction is a complicated process that considers thousands of potential scenarios and invokes various business rules based on the combination of scenarios involved. Just a few of the factors that must be considered include portability type (Inter-provider, Intra-Provider), existence of pool blocks, single-TN versus ranged-TN operations, support of optional capabilities (e.g. pseudo-LRN, optional data fields), timer settings for the involved carriers, and business hour calculations (days of the week, holidays).

The NPAC/SMS uses a complex rules engine to manage over a thousand business rules that can interact in, literally, millions of ways. Integrating a new business rule to implement a new Industry rule requires a unique mix of skills, including a deep understanding of NPAC transactions, an understanding of the specific new feature, and intimate knowledge of how the rules engine works within the NPAC/SMS to determine the impact of the new rule on existing rules. Neustar has developed this expertise over the course of many years in its role as the NPAC Administrator.

The following five business rules: timers, conflict status, first port notification, snapback, and code recovery, serve as examples of the complexity of enforcing the NPAC/SMS business rules.

Enforcement of NPAC Business Rules: Timers

The timers used by the NPAC to determine when to shift control of the port from the old SP to the new SP are referred to as the T1 and T2 timers. At the start of the T1 interval, at the end of the T1 interval (the start of the T2 interval), and at the end of the T2 interval, the NPAC generates a notification to the old SP to remind it that a pending SV has been created by the new SP and to request a reaction (concurrence or objection to the impending port). There are three sets of T1/T2 timers: two sets ("long" and "short") are selected in advance by the Service Provider. Each Service Provider selects either of the timers for port-out transactions and either of the timers for its port-in transactions. These two selections become part of the Service Provider's NPAC/SMS profile. A third set of timers, referred to as "Medium Timers" is imposed on a porting transaction when the old SP determines that the port meets the FCC's One-Day Porting criteria.

The set of T1-T2 "short" timers involves a pair of one-hour intervals and typically is selected by wireless SPs. The set of T1-T2 "long" timers involves a pair of nine-hour intervals and typically is selected by wireline SPs. The longer interval is selected by wireline SPs to accommodate the added complexity of having to assign outside plant to implement service for their customers. The medium timers are a pair of three-hour intervals. Unless the medium timer has been determined by the old SP to apply to the port, the NPAC looks at the port-out timer shown on the old SP's profile and the port-in timer shown on the new SP's NPAC profile and selects the longer to determine how long the old SP remains in control absent the old SP reacting to the NPAC/SMS notification about the pending SV creation.

The timers run during NPAC/SMS "business hours" and "business days." The NPAC/SMS is available for use at all times, except during maintenance intervals, but the timers run only during "business hours." The SP selects either Sunday through Saturday or Monday through Friday for its business days. The Sunday-Saturday business days have business hours of 9:00 a.m. to 9:00 p.m., in the predominant time zone of the region. The Monday-Friday business days have business hours of 7:00 a.m. to 7:00 p.m., Central time. The SP's selection of business days/hours is noted on its NPAC profile. The business days/hours choice is independent of the short/long timers choices. Wireline SPs typically choose the Monday-Friday set while wireless SPs typically chose the Sunday-Saturday set.

When a port meets the FCC's criteria for a One-Day Port, the old SP invokes the medium timers, indicating the choice when it submits its matching "pending SV create" request to NPAC/SMS. The NPAC then ignores the business days/hours and long/short timer settings on the NPAC/SMS profile for the two SPs involved in the port and uses the medium timers:

- T-1/T-2 timers are each three hours
- Business days are Monday through Friday
- Business hours are 7:00 a.m. to midnight, in the region's predominant time zone

The new SP is not obligated to request a next day due date even though the One-Day Porting scenario requires that it be allowed.

Enforcement of NPAC Business Rules: Conflict

When the new SP sends its "create pending SV" request to the NPAC/SMS, the NPAC/SMS sends a notification to the old SP. Thus if the LSR never made it to the SP actually serving the number, the NPAC/SMS notification serves as an alert that something is wrong. Likewise, if the old SP received the LSR, but has not issued its FOC, the NPAC/SMS notification serves as an alert that a port is being planned even without a FOC having been issued. Because the old Service Provider now is aware of the porting record being created in the NPAC/SMS, the old SP may have time to prevent or at least delay the port until it can contact the new SP to work out the problem.

The NPAC/SMS process allows the old Service Provider to a put a pending port into "Conflict", thus preventing the new Service Provider from activating the port for 6 hours (or sooner, if the old SP removes the conflict). In cases where there has been no LSR received or no FOC issued, the old SP can put the pending SV record into conflict and prevent activation for an indefinite period. The design of the NPAC/SMS enforces the Industry's rules allowing the old SP to retain control of a port for a defined interval. The delay interval values also are defined by Industry.

In addition to the T1-T2 timer process described above, the old SP can extend its control of a port by setting the conflict flag in its "old SP pending SV create" message to "false." For both long and short timer cases, this extends the interval by six hours from the time NPAC/SMS receives the conflict indication. If the port involves a "medium timers" scenario, this extension is 2 hours. Once the interval expires, the new SP can remove the conflict and proceed with the port.

On occasion, the new SP may send its LSR to the wrong old SP or may fail to send it altogether. Should that new SP attempt to create a pending SV record, in anticipation of porting a telephone number away from the old SP, the NPAC/SMS (routinely) sends a notification to the old SP to say that a pending SV has been created and to request the corresponding old SP "create pending SV request" message be generated. The old SP, realizing no LSR was received, can send its matching "create pending SV" request with conflict indicated and the conflict "cause code" marked "50" (no LSR received). These indicate to the NPAC/SMS that the pending SV should be placed into a Conflict state and remain there until the old SP removes the conflict. The same conflict sequence could occur if the scenario were that the old SP received the LSR, but had not yet issued its FOC. In this case, the conflict cause code would be "51" (no FOC issued).

Enforcement of NPAC/SMS Business Rules: First Port Notification

Some SPs do not establish translations in their networks when an NPA-NXX code is defined as portable and instead wait for the first port to occur in the NPA-NXX (or for the first thousand block to be created and assigned to a switch different from the one to which the NPA-NXX is assigned). The NPAC/SMS broadcasts a first-port notification when it receives the "create pending SV" request and prevents activation of the SV or block for five business days. The Industry requires this delay to enable those carriers that have not yet prepared their network to recognize the NPA-NXX code is portable to update their switch translators and begin doing data base dips for calls to numbers in the code.

Enforcement of NPAC/SMS Business Rules: Snapback

When a consumer abandons a number he has ported, the current SP is not permitted to use the number for another of its customers and must return it to the original SP, after providing intercept services. This is called snapback. This is accomplished by deleting the NPAC/SMS record of the ported number. When a ported number record is deleted, the NPAC/SMS notifies the code-assignee (or block assignee, if a pooled block is involved) that the number is being returned to its inventory. The NPAC message includes the date the number was removed from active service, as indicated to the NPAC/SMS by the SP returning the number, thus enabling the code (or block) assignee to apply an appropriate aging interval. After the snapback message is sent, the NPAC/SMS broadcasts a delete message to all the LSMSs.

Enforcement of NPAC/SMS Business Rules: Code Recovery

The introduction of LNP has also impacted the NPA-NXX code recovery process, where a code is assigned to a Service Provider and then later is returned to the NANPA code pool. Before the introduction of LNP, a recovered code was not contaminated, i.e., all 10,000 telephone numbers associated with it would be available for use by the next code assignee. However, a code that is defined as portable, or pooling enabled, that is recovered after it has been assigned, is likely to have had numbers ported from it. If the code is returned to the NANPA, and no action is taken to clear out the ported number records, the recovered code will not be pristine. When the code is later re-assigned, the new code assignee inadvertently may cause double assignments of telephone numbers that already are in service as ported numbers served by other SPs. To protect the code recovery process, the NPAC/SMS will not allow deletion of network data when subordinate TN-level data exists, i.e., when there are ported numbers. Contaminated NPA-NXX codes are not returned to the NANPA pool until the NPAC's telephone number-level records are cleaned out. Because code recovery often involves a defunct SP, there may be no one available to agree to the deletion of the defunct SP's NPAC/SMS records. In these cases, the NANPA obtains written direction from the state regulator, requesting that the NPAC delete the defunct SP's code record and any associated records that must be deleted to allow the code's deletion. As a result of the NPAC's action, the recovered code contains the full 10,000 numbers for use by the new code-assignee when the code eventually is reassigned.

Data Validation

Beyond enforcing Industry-defined porting processes, the NPAC/SMS validates the data it receives before completing the transaction and making the data available for dissemination. Data validations can be divided into format validations, verifying that format of the data provided conforms to Industry practices, and relationship validations, verifying the data provided against other NPAC data, Industry standards, and data from other sources such as NECA and NANPA.

Data Validation: Format Validations

One type of format validation verifies the structure of the data; specifically number or characters and whether they are numbers letters or both. Examples are an LRN, which must be 10 numeric characters; an NPA-NXX code, which must be 6 numeric characters; a Destination Point Code, which must be 9 numeric characters; and a SPID, which must be 4 alphanumeric characters.

Another type of format validation involves compliance with Industry rules, such as confirming a Subsystem Number is present when a Destination Point Code is present or that the Destination Point Code entry conforms to common channel signaling (SS7) address range restrictions.

Data Validation: Relationship Validations

Relationship validations involve verifying the data provided against existing data, such as whether the LRN entered on the ported number record exists and is associated with the New Service Provider involved in the record. Other examples are whether the value entered in the AltSPID or Last AltSPID field is a valid SPID in the NPAC's customer data, whether the value entered as the SV Type is among the defined SV Type values, and whether the NPA-NXX of the porting telephone number shown on the record exists in the NPAC's network data.

Somewhat more complex relationship validations involve confirming the SPID from which the number is being ported actually is the Service Provider currently serving the telephone number. This validation requires the NPAC/SMS to determine whether there is a ported number record already for the telephone number and, if so, to confirm the SPID associated with that record represents the "porting from" Service Provider shown on the "porting to" Service Provider's port request. If no ported number record exists, the NPAC/SMS then must check to see whether the telephone number is part of a thousand block associated with the "porting-from" Service Provider's SPID. And failing to find such a thousand block record, the NPAC must then determine whether the telephone number's NPA-NXX code is associated with the "porting from" Service Provider's SPID.

More complex validations check for relationships such as whether the Destination Point Code used is among those the Service Provider has listed as its valid DPC codes for use on its NPAC/SMS records. Another of these complex validations occurs when a Service Provider attempts to open an NPA-NXX code in the NPAC/SMS network data. Before the code can be opened, the NPAC/SMS determines to what Operating Company Number (OCN) the North American Numbering Plan Administrator (NANPA) has assigned the NPA-NXX code. That OCN then is compared with the list of OCNs associated with the SPID of the Service Provider attempting to open the code. The NPAC/SMS also confirms the code is being opened in the proper region. In two NPAC regions, this proper-region determination must be done at the rate area level because the regional boundary does not exactly track the state boundary, making it necessary to handle one NPA in two regions. Table 1.2.2-1 provides a summary of some of the validations performed by the NPAC/SMS.

Table 1.2.2-1. Examples of Validations

Field	Validation
Simple Format Validation	
[redacted]	[redacted]
NPA-NXX	must be 6 numeric characters
[redacted]	[redacted]
SPID	must be 4 alpha numeric
Compliance with Industry Rules	
[redacted]	[redacted]
SSN	when present, must be 000
[redacted]	[redacted]
First port in NPA-NXX	5 business day delay before activation permitted
[redacted]	[redacted]
LRN	must be network data owned by new SP
[redacted]	[redacted]
Last altSPID	must exist as SPID in customer data
[redacted]	[redacted]
NPA-NXX	must be open in network data
[redacted]	[redacted]
DPC	must be known to be valid for SP creating record
[redacted]	[redacted]
NPA-NXX	allow open only in region serving the NPA *
Network Data Relationships Tracked	
[redacted]	[redacted]
DPCs	DPCs associated with a SPID

Field	Validation
[redacted]	[redacted]
NPA-NXX-X	NPA-NXX-Xs associated with a SPID
[redacted]	[redacted]
LATA	LATA associated with each NPA-NXX
[redacted]	[redacted]
SP Type	each SPID's SP type
[redacted]	[redacted]

** NPAC region boundary crosses state line in Kentucky, so proper region to open an NPA-NXX code is validated at the rate area level*

Dissemination of Data

Once the NPAC/SMS has applied its processing rules on a request and updated its internal database, it must disseminate this information to the LSMS and SOA systems. Real-time broadcasting is the primary mechanism for this dissemination. Most broadcasts are sent to the subtending LSMSs, though some go to the SOAs as well.

During the porting process, the NPAC/SMS acts as a hub, connecting pairs of Service Providers (SPs) that are coordinating the transfer of a telephone number. As each party performs a step in the process, the NPAC/SMS issues real-time notifications to their SOA systems to keep all parties abreast of the progress and make them aware of their obligations. Notifications are issued for object creation (port initiation), attribute value changes, status changes, and timer expirations. Though most NPAC/SMS messages to SOAs involve information pertinent to a single SOA, some NPAC/SMS transmissions are broadcasts to all SOAs; for example, the creation of SPIDs, NPA-NXXs, and the dash-X representation of pooled blocks.

NPAC/SMS users connect a system called a Local Service Management System (LSMS) for receiving and propagating NPAC/SMS transactions in their systems and networks. NPAC/SMS transactions are updates to the Industry on changes in status related to telephone numbers. These changes in status can be a move from one switch to another, one Service Provider to another, information for a non-ported TN different from that associated with the TN's NPA-NXX code, assignment of numbering resources (pooled bocks, NPA-NXX codes) to a Service Provider, as well as hundreds of other status changes. Once a transaction is validated and updated in the NPAC/SMS database, a broadcast of the SV is sent to NPAC/SMS users through the LSMS interface. The Service Provider's LSMS updates network databases and operations support systems. They can also distribute the data in turn to their clients, such as smaller SPs that cannot justify operating an LSMS system.

In the case of an NPA split, the NPAC/SMS broadcasts an "add" of the new-NPA versions of the NPA-NXX codes impacted by the NPA split when the split is entered into the NPAC/SMS. At the end of the Permissive Dialing Period, the NPAC/SMS broadcasts a "delete" of the old-NPA versions of the NPA-NXX codes impacted by the NPA split.

Synchronization

One can think of the LNP Ecosystem as fundamentally a complex distributed database. The NPAC/SMS itself maintains the master copy of the LNP data and one of its primary goals is to ensure that remote systems have an accurate copy of that data. To this end, synchronization with remote systems is critical and the NPAC/SMS provides many layers of mechanisms to ensure consistency.

Synchronization: Recovery

Local systems are not always online, and from time to time are not able to process messages correctly due to a variety of platform issues. The NPAC/SMS implements a feature called recovery that allows a local system to retrieve messages they have missed due to such a problem. The recovery process can be done for a specific time frame, or the system can ask the NPAC/SMS to deliver accumulated message that it has missed (this is called "Send What I missed" or SWIM recovery).

new

In the Security-Related Information rather than using recovery, the NPAC/SMS will retransmit messages that either could not be delivered or were not responded to. This simplifies the interface, reducing the burden on local system implementers.

Synchronization: Failed Lists and Resend

When an SV or pooled block broadcast is received by an LSMS, it sends an acknowledgement to the NPAC/SMS. The NPAC/SMS keeps track of the LSMS responses for each broadcast. After a predefined interval, any LSMS that has not acknowledged the broadcast is placed on a "failed list." Each night, during a period of low transaction volume, the NPAC/SMS resends the broadcast to any LSMS that is on the failed list. For modify broadcast failures, the NPAC/SMS notes whether the LSMS failure was due to a "no record" rejection and for those casts sends a create message rather than rebroadcasting the modify transaction.

Synchronization: Bulk Data Downloads

Bulk Data Downloads (BDD) provides data extracts from the NPAC/SMS to local systems requesting them. Local systems retrieve the BDD files from the NPAC/SMS and can use the files to validate their own database, re-populate their database after a loss of data, or build the initial database for a new system.

There are several different types of BDD files, based on the type of data they represent. There are BDD files for Subscription Versions, Pooled Blocks, DashX, NPA-NXX, LRN, and Service Provider. For each of these files, the BDD can be generated with an "active view" that includes currently active objects, or with a "latest view of activity" that captures all activity (including deletions and modifications) within a specified time frame.

We also provide a BDD for SOA notifications. This is available based on a specific time-frame and contains only notifications for the provider requesting the data.

Synchronization: Audits

The NPAC/SMS also supports audits of the LSMSs. With the audit feature, the NPAC/SMS queries one or more LSMSs, and compares the results of these queries with its own data, issuing corrective downloads as necessary. Audits can be initiated for a single TN, a TN range, or for a time range, and can be initiated by a SOA system or by the NPAC Administrators. The NPAC/SMS issues random audits as part of its housekeeping processing as a pro-active consistency measure.

Synchronization: Query

Users can initiate queries to the NPAC/SMS and use the results to reconcile their systems. Responses are provided immediately. Queries can be for any data in the NPAC/SMS including TNs, ranges of TNs, SPIDs, DPC/SSNs, etc.

Facilitation of Industry Processes and Obligations

Because the NPAC/SMS is an authoritative database for TN administration it must support various functions that impact numbering as well as various entities that rely on numbering data. The NPAC/SMS has software that supports:

- Mergers and acquisitions of communications companies—SPID migrations
- Area code splits—recognition of dual NPAs for TNs
- Reseller identification—altSPID, last altSPID
- Administrative services that rely on NPAC—LEAP and WDNC
- IP routing—URI

Mergers and Acquisitions

The NPAC/SMS facilitates mergers and acquisitions through SPID migrations, a process that allows the SPID associated with the ported telephone numbers, thousand blocks, LRNs, and NPA-NXX codes to be changed without requiring that the data be broadcast to the LSMSs. Instead, the NPAC/SMS distributes information that allows the migrating records to be identified. The record changes are then made independently by each SOA and LSMS operator and by the NPAC/SMS during a regular NPAC/SMS maintenance window.

The NPAC/SMS offers on-line tools for both Service Providers and NPAC Administrators to define and manage these migrations. The tool implements the workflow of the migration, ensuring that both Service Providers in the migration have concurred with the activities. During the concurrence phase, automated e-mails are sent directly to the involved providers. After the migration is approved, automated emails are sent to all providers. The system also automatically validates the migration on a daily basis, and generates preliminary data files, making them available for providers at the FTP site. On the date of the migration, the system automatically cancels any pending subscription versions involved in the migration, provides reports to SPs impacted by the cancelled SVs, initiates message delivery and data updates for on-line migrations, and delivers files to Service Providers' FTP sites with instructions for handling the SPID migration off-line.